AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Arkansas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Microsoft Skype account for "live:m43767"

Case No. 5:18CM 51

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See "Attachment A"

located in the Western District of Arkansas, there is now concealed *(identify the person or describe the property to be seized)*:

See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A	Computer Child Pornography

The application is based on these facts:

See "Attachment C"

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Gerald Faulkner, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/15/18

Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Microsoft Skype user name / user ID:

"live:m43767"

between the time period of November 1, 2017 until the present

that is stored at premises owned, maintained, controlled, or operated by Microsoft, Incorporated - Online Operations / Microsoft Skype headquartered at One Microsoft Way in Redmond, Washington 98052

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Skype

To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft, Incorporated. ("Skype"), including any messages, records, files, logs, or information that have been deleted but are still available to Microsoft Skype. Microsoft Skype is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Skype passwords, Skype security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other activities;

(c) All photos and videos uploaded, distributed, received, or saved by that user ID;

(d) All profile information, status updates, and contact lists associated with the accounts;

(e) All other records of communications and messages made or received by the user;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All past and present lists of friends or contacts created by the account;

(i) Any and All information deleted from the accounts but still recoverable by Microsoft Skype;

(j) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(k) All privacy settings and other account settings, including privacy settings;

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2251 and Section 2252 involving the suspects outlined herein since **November 1, 2017 until present**, including, for each user ID identified on Attachment A, information pertaining to the following matters:

(a) Included, but not limited to, any and all sexually explicit images of minors

(b) Evidence indicating how and when the Microsoft Skype account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Microsoft Skype account owner;

(c) Evidence indicating the Microsoft Skype account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to the sexual exploitation of children or involving nude images of children being sent and received via the Internet or other means.

(f) Any and all conversations, contacts, messages, emails, posts and/or chats involving the solicitation or enticement of minors to engage in sexually explicit conduct and/or encouraging minors to produce images or videos of themselves nude or engaging in sexually explicit conduct. Any and all conversations with others, adult or minors, concerning the sexual exploitation of children or the sending or receiving of images of minors, nude, clothed, or otherwise.

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS :
:
: **ss. AFFIDAVIT**
:
COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

I, Gerald F. Faulkner, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with HSI since April, 2009. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants and arrest warrants, a number of which involved child exploitation and/or child pornography offenses. This affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

2. This affidavit is made in support of applications for a search warrant for information associated with certain accounts that are stored at a premises owned, maintained, controlled, or operated by Microsoft, Incorporated - Online Operations / Microsoft Skype, an

electronic telecommunications service provider headquartered at One Microsoft Way in Redmond, Washington 98052. This affidavit is made in support of an application for a search warrant under Title 18, United States Code (U.S.C.) §§ 2252A, relating to possession, distribution and production of images/videos of child pornography; to require Microsoft, Incorporated – Online Operations / Microsoft Skype to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with Microsoft Skype user account of **"live:m43767".**

3. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft, Incorporated – Online Operations / Microsoft Skype to disclose to the government the requested records and other information in its possession. As such, your Affiant is requesting authority to search the social media accounts where the items specified in Attachment A may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

4. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code (U.S.C.) § 2252A, relating to possession, distribution and production of child pornography, are presently located within the Microsoft Skype user account of **"live:m43767"**. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

5. This investigation, described more fully below, has revealed that the individuals using the Microsoft, Incorporated – Online Operations / Microsoft Skype user account **"live:m43767"**, have been created and utilized to distribute images/videos of child pornography in violations of Title 18, United States Code, Sections 2252A.

Statutory Authority

6. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

a. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person's interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

Background Regarding Computers and the Internet

7. Your Affiant has become familiar with the Internet, which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state.

8. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail") or Instant Messaging services (IM). An individual who wants to use the Internet must first obtain an account with a computer or cellular telephone that is linked to the Internet – for example, through a commercial service – which is called an "Internet Service Provider" or "ISP". Once the individual has accessed the Internet, whether from a residence, a university, a place of business or via their

cellular service provider, that individual can use Internet services, including sending and receiving e-mail and IM.

9. The Internet is a worldwide computer network that connects computers and facilitates the communication and the transfer of data and information across state and international boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 12.345.678.901. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

10. Computers as well create a "Log File" that automatically records electronic events that occur on the computer. Computer programs can record a wide range of events including remote access, file transfers, long/logoff times, systems errors, Uniform Resource Locator addresses (websites), unique searches performed on the Internet and various forms of electronic communications.

11. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto the hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is

overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

12. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

13. The use of the Internet and more specifically electronic communications via the Internet provides individuals the ability to mask their true identities as well as their physical locations. Additionally, the use of the Internet provides individuals and their associates the ability to access social networking sites free of charge to further their criminal activity

Background Regarding Microsoft Skype Accounts

14. Based on my knowledge and experience and information obtained from other law enforcement personnel with training and experience in this area, the following is known about Microsoft Skype Accounts:

a. Microsoft Skype is a telecommunications application software product that specializes in providing video chat and voice calls between computers, tablets, mobile devices, the Xbox One console and smartwatches via the Internet.

b. Microsoft Skype additionally provides instant messaging services and users may transmit both text and video messages. Users may also exchange digital documents such as images, text and video.

c. Microsoft Skype allows users to communicate over the Internet by voice using a microphone, by video using a webcam and by instant messaging.

d. Registered users of Microsoft Skype are identified by a unique Skype name and may be listed in the Skype directory. Skype allows registered users to communicate through both instant messaging and voice chat.

e. Microsoft Skype supports conference calls, video chats and screen sharing between twenty-five (25) users at a time for free.

Summary of the Investigation to Date

15. In March 2018, your Affiant received seven (7) Cyber Tip Line Reports, Numbers 26291872, 26295314, 26295441, 26296474, 26296558, 26296577 and 26296887 from the National Center for Missing and Exploited Children (NCMEC) in reference to media files containing what was believed to be child pornography being uploaded onto a Microsoft Skype user profile account.

16. The information on the suspected media files containing child pornography were submitted to the Cyber Tip Line by Microsoft, Incorporated with all incident dates occurring on December 11, 2017. The incident information was categorized as being "apparent child pornography" which was viewed and identified by Microsoft, Incorporated representatives on all associated Cyber Tips in December 2017. A total of approximately fifteen (15) uploaded images of suspected child pornography were linked to the reports.

17. Microsoft, Incorporated provided the Cyber Tip Line with the following information of the user being reported:

Screen/User Name: **live:m43767**
Number of Files: 15
Type: Upload
Date Range: 12/11/17
IP Addresses: 70.178.186.187 and 174.255.137.110

18. Your Affiant viewed all of the files linked to the Cyber Tip Line Report Numbers and determined the majority of them to in fact be images of child pornography. On April 17, 2018, your Affiant again viewed and described three (3) of these files as follows:

(a) **Screen/User Name: live:m43767**
IP Address: 70.178.186.187
Date/Time: 12/11/17 20:31:00 UTC
Filename: 487a2dbc-53e8-4da7-a907-d59286dbe57b.jpg

This image is of an approximate four (4) to six (6) year old prepubescent female with her underwear pulled down and an adult male's hand holding open her vagina and anus open. The prepubescent female's vagina and anus are exposed to the camera. The adult male's thumb is placed next to the prepubescent female's vagina and the length from his knuckle to fingertip is approximately larger than the entire vagina assisting in the development determination of the minor child.

(b) **Screen/User Name: live:m43767**
IP Address: 174.255.137.110
Date/Time: 12/11/17 16:23:10 UTC
Filename: 4dc991f5-e0ce-4178-a584-1e4496f74da0.jpg

This image is of an approximate eight (8) to ten (10) year old prepubescent female completely naked laying on bed with her legs spread and her hand placed on her vagina. The minor child's anus and breasts are also exposed to the camera.

(c) **Screen/User Name: live:m43767**
IP Address: 174.255.137.110
Date/Time: 12/11/17 16:23:10 UTC
Filename: 95f2fab8-1480-47e4-9d09-9f85d1461eec.jpg

This image is of an approximate seven (7) to nine (9) year old prepubescent female completely naked sitting on what appears to be a chair with her legs spread back towards the rear of the chair. The minor's child vagina and breasts are exposed to the camera.

19. Your Affiant conducted DHS and open source database queries which revealed the IP address 174.255.137.110, documented in the multiple uploads of child pornography through the Microsoft Skype Screen/User "**m43767**" was registered through Verizon Wireless Telecommunications Company. Documents received on or about April 12, 2018 from Verizon Wireless Telecommunications Company in reference to IP address 174.255.137.110 revealed the IP to be a Natting Router IP address (can have many users at the same time associated to the same IP). Attached with the returned documents from Verizon Wireless Telecommunications Company was a spreadsheet with all cellular telephone numbers linked to that Natting Router IP address at the requested times on December 11, 2017. Your Affiant reviewed the spreadsheet and located a specific cellular telephone number, namely 479-445-0387, reflecting a Northwest Arkansas area code.

20. DHS database queries revealed the cellular telephone number 479-445-0387 was linked to a June 2016 arrest report through the Washington County, Arkansas Sheriff's Office for Arkansas State Charges of Rape-Forcible Fondling. The suspect of the alleged charges was listed as being Michael KOONTZ with a home address of 443 Tower Lane in Winslow, Arkansas and a contact cellular telephone number of 479-445-0387.

21. On April 26, 2018, at approximately 0600 hours, pursuant to the ongoing child exploitation investigation, HSI Special Agents and Task Force Officers (TFO) assigned to the Internet Crimes Against Children (ICAC) Task Force arrived at the residence of Michael KOONTZ located at 443 Tower Lane in Winslow, Arkansas to execute a federal search warrant for possible violations of Title 18, United States Code, Sections 2252A – Possession/Distribution of Child Pornography.

22. KOONTZ was encountered during the execution of the federal search warrant and in a post-Miranda interview stated he currently has Cox Communications as their internet service provider with secured, password protected wireless internet. Your Affiant questioned KOONTZ

about his cellular service provider to which he replied it was believed to be through Straight Talk Wireless and his personal cellular telephone number was 479-445-0387.

INVESTIGATORS NOTE: Straight Talk Wireless is a type of carrier known as a Mobile Virtual Network Operator (MVNO), which means that it doesn't run or own a wireless network. Instead, it purchases the right to use towers from AT&T, T-Mobile, Verizon and Sprint. The personal cellular telephone number KOONTZ provided is one in the same cellular telephone number associated to the Skype Screen/User "**m43767**" recorded through the Natting Router IP address with Verizon Wireless Telecommunications Company.

23. Your Affiant informed KOONTZ about the multiple Cyber Tip Line Report leads received from the NCMEC involving a Skype user of "**m43767**" having uploaded numerous images of child pornography. KOONTZ stated the "**m43767**@gmail.com" email was probably the one he had set up through his wife's account and was also probably the same one he set up for his Skype account. KOONTZ was told approximately fifteen (15) images of child pornography had been uploaded from his Skype account onto the internet. He stated if there was any child pornography on that account he would have obtained it through "Fantasti.cc" and "Smutty.com" where users on those sites would post images of child pornography. KOONTZ further explained there was an unknown user on Skype that would have requested these child pornography images and KOONTZ would find them through "Smutty.com" and then send them upon request. Your Affiant then clarified with KOONTZ the federal definition of child pornography to where it would pertain to naked images of minor children with their breasts and vaginas exposed or engaged in sexual activity. KOONTZ replied, "on those, they claim to be of eighteen (18) but I seriously doubt it". Your Affiant informed KOONTZ he had personally viewed the images of child pornography uploaded from his Skype account and those images were not of age difficult determination minor females. KOONTZ said there were two or three users on "Smutty.com" who would post images of child pornography through the private messaging and if anyone on Skype would have requested photographs of that nature he would send them. ICAC TFO Leon Frisard asked KOONTZ if his online actions could better be described as him obtaining images of

child pornography through the "Smutty.com" website from unknown users and then saving them to his cellular telephone and then sending them upon request to unknown Skype users via the private messaging application. KOONTZ admitted that was how these images were being uploaded onto his Skype account but initially he was not saving the images of child pornography he would see on "Smutty.com". He explained he started saving the viewed images of child pornography when the unknown users on Skype started asking for pictures of that nature.

Conclusion

24. Based on the foregoing information, probable cause exists to believe there is located on the computer servers of Microsoft, Incorporated - Online Operations / Microsoft Skype headquartered at One Microsoft Way in Redmond, Washington 98052 evidence of violations of Title 18, United States Code, Section 2252A. Your Affiant prays upon this honorable court to issue a search warrant to Microsoft, Incorporated – Online Operations / Microsoft Skype for the items set forth in attachment "B" (which is attached hereto and incorporated herein by reference), that constitute evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Sections 2252A.

Gerald Faulkner, Special Agent
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 15th day of May 2018

Erin L. Wiedemann
United States Magistrate Judge